HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,387	03/29/2001	Lebin Cheng	10010859-1	7378

7590 03/07/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,387	CHENG, LEBIN	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-20 have been reconsidered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1,2-4,13-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett, U.S. Patent No. 5,968,176, in view of Hind, U.S. Patent No. 6,585,778.

As per claims 1 and 20, the applicant describes a method of configuring a network security system comprising the following limitations which are met by Nessett in view of Hind:

a) forming a registry data structure for defining roles within a network (Nessett: Col 5, lines 27-37);

b) mapping network security policies to the registry data structure, said network security policies being contained in one or more policy documents, the one or more policy documents being in a standard document format language (Nessett: Col 4, lines 10-14; Col1 24, lines 38-40; Hind: Col 3, lines 46-67);

c) using a document transformation algorithm to transform the policy documents into one or more device-specific configuration documents stored in machine-readable form (Nessett: Col 4, lines 14-20);

Nessett discloses all the limitations of original claims 1 and 20 as rejected in the first office action. The additional limitation of "the one or more policy documents being in a standard format language" is met by Hind.

Nessett discloses that his security policies are stored in security policy statements. The security policy statements are security policy documents. Though Nessett does not reference a particular language which the policy statements are written in, he does disclose that a transformation algorithm exists which "translates the security policy statements into configuration data in the formats needed for nodes in the network" (Col 4, lines 16-18). Thus Nessett satisfies the goal of scalability as disclosed by the applicant because documents are transformed into end target specific formats.

Nessett, however, does not disclose the particular language which the security policy statements are written in. Hind discloses a system which enforces data policy through the use of security policies stored as XML documents. Furthermore, Hind discloses that XML is widely adopted as an industry standard for exchanging data through networks (Col 7, lines 27-33) and a good choice for storing security policies which are transformed into output documents when a policy is being enforced.

It would have been obvious to one of ordinary skill in the art at the time the invention to combine the ideas of Hind with Nessett and use XML format language for the security policy statements because XML is commonly known and used standard for the exchanging of data through networks and a good language to use in a system for enforcing data policy as disclosed by Hind.

As per claim 2, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:

further comprising generating instances of the roles and associated security policies, each instance being mapped to physical segments of the network (Nessett: Col 5, lines 50-56).

As per claim 3, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:

further comprising distributing the device-specific configuration documents to network entities for implementing the network security policies (Nessett: Col 3, lines 22-32).

As per claim 4, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:

wherein the registry data structure comprises a collection of documents that include information regarding the network roles and topology of the network (Nessett: Col 5, lines 27-37; Col 7, lines 17-20).

As per claim 13, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:.

wherein the security policies are representative of restrictions to be placed on one or more of the network roles in the registry data structure (Nessett: Col 3, lines 29-40).

The applicant should note that the management and enforcing of the security policies necessitates that restrictions would have to be placed on one or more network roles.

As per claim 14, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is also met by Hind:

Wherein the policy documents are in extensible markup language (XML) (Hind: Abstract).

As per claim 15, the applicant describes the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is also met by Hind:

Wherein the document transformation algorithm is specific to a network entity utilized for implementing one or more of the security policies contained in the policy documents (Hind: Abstract).

As per claim 16, the applicant describes the method of claim 15, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Hind and Nessett:

Wherein the document transformation algorithm includes style sheet language for transformation (XSLT) controlled by a script (Hind: Abstract; Nessett: Col 4, lines 47-51).

The use of XSLT is disclosed by Hind. The use of a script controlling the transformation algorithm is disclosed by Nessett. Reasons for combining Hind's ideas of using XML and XSLT with Nessett's system are given in the rejection for claims 1 and 20.

As per claim 17, the applicant describes the method according to claim 16, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:

wherein the script is specific to a network entity (Nessett: Col 4, lines 47-55; Col 9, lines 33-38).

As per claim 18, the applicant describes the method according to claim 16, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Nessett:

further comprising a step of selecting a script from among a plurality of scripts, each being specific to a different network entity (Nessett: Col 4, lines 47-55).

The applicant should note that Nessett discloses that depending on which script is selected, the topology data structure gives instruction as to which network entities can deal with the script. Thus, various scripts are specific to network entities.

Claims 5,6, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of Hind in further view of Mohaban, U.S. Patent No. 6,463,470.

As per claim 5, the applicant limits the method of claim 1, which is met by Nessett in view of Hind (see above), with the following limitation which is met by Mohaban:

Wherein the registry data structure comprises a hierarchy of network types, each type comprising a definition of a network role (Mohaban: Fig 8C);

Nessett in view of Hind discloses all the limitations of claim 1. However, neither Nessett nor Hind disclose how the security policies are stored. Mohaban discloses a method of storing policies in a hierarchy with each type in the hierarchy playing a network role as the policies are grouped according to domain, group, etc. Furthermore, Mohaban also discloses the use of abstract types in the hierarchy such

as the main domain (842 of Fig 8C) and the policy group (848 of Fig 8C). In Mohaban's policy hierarchy, the actual policy rules (850) are nested under a variety of abstract types.

Mohaban's hierarchy structure with abstract types and each type playing a network role provides organization to the stored policies. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Mohaban with those of Nessett in view of Hind and add a hierarchy of types that play network roles and have applications associated with them for organization and ease of looking up and retrieving the stored policies.

As per claim 6, the applicant limits the method of claim 5, which is met by Nessett in view of Hind in further view of Mohaban (see above), with the following limitation which is also met by Mohaban:

Wherein each network role is representative of a set of applications to be supported by the network (Mohaban: Fig 8C);

The applicant should note each type down the hierarchy gets more specific and the further you go down on the list the fewer applications that are supported.

As per claim 10, the applicant describes the method according to claim 6, which is rejected by Nessett in view of Hind in further view of Mohaban (see above), with the following limitation which is met by Mohaban:

Wherein at least one of the network types is an abstract type without an instance mapped to a physical network segment (Mohaban: Col 6, lines 35-47; Fig 8C);

Claims 5-9,11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of Hind in further view of The Open Group (The Open Group; "Authentication and Security Services-Introduction to Security Services"; 1997; Pages 44-56).

As per claim 5, the applicant discloses the claim limitation of claim 1, which is met by Nessett in view of Hind, with the following limitation which is met by The Open Group:

wherein the registry data structure comprises a hierarchy of network types, each type comprising a definition of a network role (The Open Group: page 56);

The Open Group illustrates how using a hierarchy to lay out a registry data structure is an effective way to store information (page 56). The hierarchy as described by The Open Group is an effective way to store information because it allows for mapping of responsibilities between a parent and its children. In this manner it allows information to be managed effectively because the information is arranged structurally. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with the ideas of Nessett and use a hierarchy of network types to effectively store information.

As per claim 6, the applicant discloses the limitation of claim 5, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by Nessett:

wherein each network role is representative of a set of applications to be supported by the network (Nessett: Col 5, lines 27-37; Col 7, lines 17-20);

Nessett discloses the use of network roles or nodes which have identifying traits such as "the type of security policy that the node is able to enforce, the constructs used to enforce policy... and connection of the node to other nodes in the network" (Col 5, lines 35-38). Nessett shows that network roles or nodes are representative of a set of applications to be supported by the network. Nessett, however, fails to specify the hierarchical framework that these roles or nodes could be placed in. The Open Group provides motivation to use a hierarchy because, as they claim, it is easy to manage data in this format. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with those of Nessett in view of Hind to have network roles, which are in a hierarchical fashion, representative of a set of applications to be supported by the network.

As per claim 7, the applicant discloses the claim limitation of claim 5, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by The Open Group:

wherein when a parent network type is mapped to a policy contained in one of the policy documents, a child network type of the parent network type inherits the policy (The Open Group: pages 44-45);

The Open Group describes a method whereby policies associated with a parent network type are mapped to an inheriting child network type (pages 44-45) for security purposes. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with the ideas of Nessett in view of Hind and map the policies of the parent network type to the child network type for security and organization.

As per claim 8, the applicant discloses the limitation of claim 7, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by The Open Group:

wherein when the child network type is mapped to a policy contained in one of the policy documents that is [in] conflict with the policy inherited from the parent, the policy mapped to the child takes precedence over the policy inherited from the parent (The Open Group: page 45);

The Open Group discloses an inheritance system whereby the child type inherits its data, such as its access control list (ACL), from the parent by default. The Open Group goes on to claim that "if any of these ACLs are specified, they override the corresponding default [to the parent]" (page 45). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined the ideas of The Open Group with those of Nessett in view of Hind to create a hierarchical system where policies mapped to a child take precedence over those mapped to a parent if specified so that a user's mapping takes precedence over default mapping.

As per claim 9, the applicant discloses the limitation of claim 5, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by Nessett:

wherein an instance of one of the network types is mapped to one or more physical network segments and wherein the network type includes a set of data fields for defining the physical network segments (Nessett: Col 3, lines 34-40);

Nessett discloses a system whereby security policies are mapped to network devices which enforce the policies: "The multilayer firewall also includes a collection of network devices that are used to enforce the defined policy. The security functions operating in this collection of network devices across multiple protocol layers are coordinated by the policy definition component so that particular devices enforce that part of the policy pertinent to their part of the network" (Nessett: Col 3, lines 34-40). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with those of Nessett in view of Hind because mapping security policies to network devices is an effective way to maintain security in a system.

As per claim 11, the applicant discloses the limitation of claim 5, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by The Open Group:

wherein each network type further comprises a data field for identifying a human administrator (The Open Group: page 56);

The Open Group discloses a hierarchical model of nodes in a security system whereby a user, or client, can manipulate the nodes by entering certain data which is recognized by the nodes (page 56). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with those of Nessett in view of Hind so that one can add a data field for identifying a human administrator to the network nodes so that they can be manipulated by a user.

As per claim 12, the applicant discloses the limitation of claim 5, which is met by Nessett in view of Hind in further view of The Open Group, with the following limitation which is met by The Open Group:

wherein each network type further comprises a data field for providing a human readable description of the network type;

The Open Group discloses a hierarchical structure of nodes in a security system whereby a client can manipulate the system by referring to a node by name (page 56). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined the teachings of The Open Group with the teachings of Nessett in view of Hind to add human readable descriptions to network types.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of Hind in further view of Kay (Kay, Michael H; XSLT Programmer's Reference, chapter "XSLT Part 2- How Does XSLIT Transform XML?"; 20 February 2001. Wrox Books).

As per claim 19, the applicant discloses the limitation of claim 16, which is met by Nessett in view of Hind, with the following limitation which is met by Kay:

wherein the device-specific configuration documents are in plain text format.

Nessett in view of Hind disclose all the limitations of claim 16. However, Nessett nor Hind discloses the particular format the documents, or statements, are output in.

Kay writes in the first paragraph, "The data structure that results from the first stage can be output as HTML, a text file or as XML... Plain text output allows data to be formatted in the way an existing application can accept". It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined the teachings of Kay with those of Nessett in view Hind and make the output format for the device-specific configurations to be plain text so that they are in an acceptable format for the applications.

Remarks to Applicant

The applicant believes that claims 1-20 should be allowable because Nessett does not disclose the use of "the one or more policy documents being in a standard document format language". Nessett's policy documents are referred to as policy statements as acknowledged by the applicant. Though a specific format language for the documents is not cited by Nessett, it is inherent in the art that the statements are written in a standard, commonly-used format language.

For clarity sake, the examiner has rejected claims 1 and 20 under 35 U.S.C. 103(a) (instead of 102(b) combining the additional reference of Hind which not only discloses that security policies are stored in a standard document format language but additionally discloses that in his system the format language is XML like in the applicant's system.

The applicant also states that there is no prior art rejection for claim 10. After the applicant's amendment clarified the scope of the claim, the examiner applied new art reference Mohaban which teaches a hierarchy organization of policies with abstract types which do not have an instance mapped to a physical network segment.

Finally, the applicant states that claims 14 and 16 should be allowable over Nessett in view of Cheung because the use of XML as discussed in Cheung may be good for E-Commerce but may not be good for a security policy system and therefore does not provide motivation for combination with Nessett's system. Claims 14-16 stand rejected on the same grounds as provided in the first office action because Cheung's article, though it deals with E-Commerce, exhibits the scalability of using XML and XSLT in a scalable distributed environment. New rejections for claims 14-16 have been rejected as these claims are also met by new reference Hind.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER